

## AMENDMENTS TO THE CLAIMS

1. (Currently amended) A terminal apparatus that communicates with another terminal apparatus on a peer to peer network, ~~the said~~ terminal apparatus possessing a public key of a group formed on the peer to peer network, said terminal apparatus comprising:

an inquiry information sending unit operable to send inquiry information to ~~said another~~ the other terminal apparatus, the inquiry information indicating an inquiry about whether or not ~~said another~~ the other terminal apparatus is a terminal apparatus of an authorized member of the group formed on the peer to peer network;

an encrypted information receiving unit operable to receive predetermined encrypted information from ~~said another~~ the other terminal apparatus in response to the inquiry information sent by ~~the said~~ inquiry information sending unit;

a decryption trial unit operable to try decrypting the received encrypted information by using the group public key;

an information judgment unit operable to make a judgment ~~on as to~~ whether or not decrypted information is appropriate ~~or not~~, only when said decryption trial unit successfully decrypts the received encrypted information ~~the decryption succeeds in the decryption trial unit~~, and the decrypted information includes a group participation certificate whose expiration date does not exceed a predetermined expiration date; and

a terminal judgment unit operable to judge that ~~said another~~ the other terminal apparatus is a terminal apparatus of an authorized member of the group, when ~~the said~~ information judgment unit judges that the decrypted information is appropriate.

2. (Currently Amended) The terminal apparatus according Claim 1, wherein:

~~the said~~ inquiry information sending unit is further add ~~operable to add~~, to the inquiry information, identification information for identifying ~~the said~~ terminal apparatus, and ~~sends~~ send the inquiry information added with ~~said the~~ identification information; and

~~the said~~ information judgment unit is further judges ~~operable to judge~~ whether or not the decrypted information includes ~~said the~~ identification information, when making the judgment ~~on as to~~ whether or not the decrypted information is appropriate ~~or not~~.

3. (Currently Amended) The terminal apparatus according to Claim 2, wherein:  
the said inquiry information sending unit is further adds operable to add, to the inquiry information, information indicating that a user of the said terminal apparatus wishes to join the group, and ~~sends~~ send the inquiry information added with ~~said~~ the information indicating that the user of said terminal apparatus wishes to join the group;  
the said information judgment unit is further judges operable to judge whether or not the decrypted information includes information indicating that the user of the said terminal apparatus is approved to join the group; and  
the said terminal judgment unit is further operable to judge ~~judges~~ that the user of the said terminal apparatus has joined the group, when the said information judgment unit judges that the decrypted information includes the information indicating that the user of the said terminal apparatus is approved to join the group.

4. (Currently Amended) The terminal apparatus according to Claim 2, wherein:  
the said inquiry information sending unit is further adds operable to add an arbitrary character string to the inquiry information, and ~~sends~~ send the inquiry information added with ~~said~~ the character string;  
the said information judgment unit is further judges operable to judge whether or not the decrypted information includes ~~said~~ the character string and a participation certificate allowing a user of ~~said~~ another the other terminal apparatus to participate in the group; and  
the said terminal judgment unit is further judges operable to judge that ~~said~~ another the other terminal apparatus is a terminal apparatus of an authorized member of the group, when the said information judgment unit judges that the decrypted information includes the character string and the participation certificate.

5. (Currently Amended) The terminal apparatus according to Claim 4, wherein:  
the participation certificate includes a specified expiration date;  
the said information judgment unit is further judges operable to judge whether or not the participation certificate included in the decrypted information is valid ~~or not~~ on the basis of ~~said~~ the expiration date; and

~~the said~~ terminal judgment unit is further operable to judge ~~judges that said~~  
~~another the other~~ terminal apparatus is a terminal apparatus of an authorized member of  
the group, when ~~the said~~ information judgment unit judges that the participation  
certificate is valid.

6. (Currently Amended) The terminal apparatus according to Claim 2, wherein:

~~the said~~ inquiry information sending unit is further operable to add ~~adds an~~  
arbitrary character string to the inquiry information, and ~~sends~~ send the inquiry  
information added with ~~said the~~ character string;

~~the said~~ information judgment unit is further judges operable to judge whether or  
not the decrypted information includes ~~said the~~ character string, a specified participation  
certificate, and a specified participation certificate issue permit; and

~~the said~~ terminal judgment unit is further judges operable to judge that ~~said~~  
~~another the other~~ terminal apparatus is a terminal apparatus of an authorized member of  
the group, when ~~the said~~ information judgment unit judges that the decrypted information  
includes the character string, the participation certificate, and the participation certificate  
issue permit.

7. (Currently Amended) The terminal apparatus according to Claim 6, wherein:

each of the participation certificate and the participation certificate issue permit  
individually includes a specified expiration date; ~~individually~~;

~~the said~~ information judgment unit is further judges operable to judge whether or  
not the participation certificate and the participation certificate issue permit included in  
the decrypted information are valid ~~or not~~ on the basis of ~~said the~~ individual expiration  
date; and

~~the said~~ terminal judgment unit is further judges operable to judge that ~~said~~  
~~another the other~~ terminal apparatus is a terminal apparatus of an authorized member of  
the group, when ~~the said~~ information judgment unit judges that both the participation  
certificate and the participation certificate issue permit are valid.

8-9. (Cancelled)

10. (Currently amended) A communication method for a first terminal to communicate with a second terminal on a peer to peer network, wherein the first terminal possesses a public key of a group formed on the peer to peer network, ~~the said~~ communication method comprising:

an inquiry information sending step of sending inquiry information to the second terminal, the inquiry information indicating an inquiry about whether or not the second terminal is a terminal of an authorized member of the group formed on the peer to peer network;

an encrypted information receiving step of receiving predetermined encrypted information from the second terminal in response to the inquiry information sent in the said inquiry information sending step;

a decryption trial step of trying to decrypt ~~decrypting~~ the received encrypted information by using the group public key;

an information judgment step of making a judgment ~~on as to whether or not~~ decrypted information is appropriate or not, only when the said decryption trial step successfully decrypts the received encrypted information, succeeds in the decryption trial step and the decrypted information includes a group participation certificate whose expiration date does not exceed a predetermined expiration date; and

a terminal judgment step of judging that the second terminal is a terminal of an authorized member of the group, when the decrypted information is judged to be appropriate in ~~the said~~ information judgment step.

11. (Currently Amended) The communication method according to Claim 10, wherein;

~~in the said inquiry information sending step comprises adding~~ identification information for identifying the first terminal ~~is added to the inquiry information, and sending the inquiry information added with said the identification information is sent; and~~

~~in the said information judgment step, it is further judged comprises judging~~ whether or not the decrypted information includes ~~said the~~ identification information for

identifying the first terminal, when the judgment is made on whether or not the decrypted information is appropriate ~~or not~~.

12. (Currently Amended) The communication method according to Claim 11, wherein;

~~in the~~said inquiry information sending step comprises adding; information indicating that a user of the first terminal wishes to join the group ~~is added to the inquiry information, and~~ sending the inquiry information added with said the information indicating that the user of the first terminal wishes to join the group;~~is sent;~~

~~in the~~said information judgment step, ~~it is further judged~~ comprises judging whether or not the decrypted information includes information indicating that the user of the first terminal is approved to join the group; and

~~in the~~said terminal judgment step, ~~it is further judged~~ comprises judging that the user of the first terminal has joined the group, when said information judgment step judges that the decrypted information is judged, in the information judgment step, to include~~includes~~ the information indicating that the user of the first terminal is approved to join the group.

13. (Currently Amended) The communication method according to Claim 11, wherein;

~~in the~~said inquiry information sending step, comprising adding an arbitrary character string ~~is further added to the inquiry information, and~~ sending the inquiry information added with said the character string;~~is sent;~~

~~in the~~said information judgment step comprises judging; ~~it is further judged~~ whether or not the decrypted information includes ~~said the~~ character string and a participation certificate allowing a user of the second terminal to participate in the group; and

~~in the~~said terminal judgment step, ~~it is further judged~~ comprises judging that the second terminal is a terminal of an authorized member of the group, when said information judgment step judges that the decrypted information is judged, in the

~~information judgment step, to include~~ includes the character string and the participation certificate.

14. (Currently Amended) The communication method according to Claim 13,

wherein:

the participation certificate includes a specified expiration date;

~~in the~~ said information judgment step, ~~it is further judged~~ comprises judging whether or not the participation certificate included in the decrypted information is valid ~~or not on the basis of said~~ the expiration date; and

~~in the~~ said terminal judgment step, ~~it is further judged~~ comprises judging that the second terminal is a terminal of an authorized member of the group, when said information judgment step judges that the participation certificate is judged to be valid in the information judgment step.

15. (Currently Amended) The communication method according to Claim 11,

wherein;

~~in the~~ said inquiry information sending step, ~~an~~ comprises adding an arbitrary character string ~~is further added to the inquiry information; and~~ sending the inquiry information added with ~~said the~~ character string; ~~is sent;~~

~~in the~~ said information judgment step, ~~it is further judged~~ comprises judging whether or not the decrypted information includes ~~said the~~ character string, a specified participation certificate, and a specified participation certificate issue permit; and

~~in the~~ said terminal judgment step, ~~it is further judged~~ comprises judging that the second terminal is a terminal of an authorized member of the group, when said information judgment step judges that the decrypted information is judged, in the information judgment step, to include includes the character string, the participation certificate, and the participation certificate issue permit.

16. (Currently Amended) The communication method according to Claim 15,

wherein;

each of the participation certificate and the participation certificate issue permit individually includes a specified expiration date; ~~individually,~~

~~in the said~~ information judgment step, ~~it is further judged~~ comprises judging whether or not the participation certificate and the participation certificate issue permit included in the decrypted information are valid ~~or not~~ on the basis of ~~said the~~ individual expiration date; and

~~in the said~~ terminal judgment step, ~~it is further judged~~ comprises judging that the second terminal is a terminal of an authorized member of the group, when said information judgment step judges that both the participation certificate and the participation certificate issue permit are ~~judged to be valid in the information judgment~~ step.

17-18. (Cancelled)

19. (Currently Amended) A communication method for carrying out a communication between a first terminal and a second terminal on a network, wherein the first terminal possesses a public key of a group formed on the network and a pair of a private key and a public key of a first user who is a user of the first terminal, and the second terminal possesses a pair of a private key and a public key of the group, ~~the said~~ communication method comprising steps A executed by the first terminal and steps B executed by the second terminal,

wherein ~~the said~~ steps A include:

an inquiry information sending step of sending inquiry information to the second terminal, the inquiry information indicating an inquiry about whether or not the second terminal is a terminal of an authorized member of the group;

an encrypted information receiving step of receiving predetermined encrypted information from the second terminal in response to the inquiry information sent in ~~the said~~ inquiry information sending step;

a decryption trial step of trying ~~decrypting to decrypt~~ the received encrypted information by using the group public key;

an information judgment step of making a judgment ~~on~~ as to whether or ~~not~~ not decrypted information is appropriate ~~or not~~, when said decryption trial step successfully decrypts the received encrypted information ~~the decryption succeeds in the decryption trial step~~;

a manager judgment step of judging that the second terminal is a terminal of an authorized manager of the group, when the decrypted information is judged to be appropriate in the information judgment step;

a membership request sending step of sending membership request information to the second terminal judged to be the authorized manager in ~~the~~ said manager judgment step, the membership request information including information indicating that the first user wishes to join the group and the public key of the first user; and

a participation certificate receiving step of receiving a participation certificate indicating that the first user has been approved to join the group from the second terminal; and

~~the~~ wherein said steps B include:

an inquiry information receiving step of receiving the inquiry information from the first terminal;

an encrypted information sending step of generating the encrypted information which has been encrypted according to the received inquiry information, and sending the generated encrypted information to the first terminal;

a membership request receiving step of receiving the membership request information from the first terminal;

a participation certificate generation step of generating the participation certificate on the basis of the received membership request information; and

a participation certificate sending step of sending the generated participation certificate to the first terminal.

20. (Currently Amended) The communication method according to Claim 19, wherein ~~the~~ said steps B further include:



a request date specification step of specifying a date, month and year on which the membership request information was received; and

an expiration date determination step of determining an expiration date of the participation certificate on the basis of ~~said~~the specified date, month, and year; and

wherein said in the participation certificate generation step comprises generating; the participation certificate is ~~generated~~ according to the membership request information and ~~said~~the expiration date.

21. (Currently Amended) A communication method for carrying out a communication between a first terminal and a second terminal on a network, wherein the first terminal possesses a pair of a private key and a public key of a group formed on the network and a public key of a second user who is a user of the second terminal, and the second terminal possesses a public key of the group, ~~the~~said communication method comprising steps A executed by the first terminal and steps B executed by the second terminal,

wherein ~~the~~said steps A include:

an inquiry information sending step of sending inquiry information to the second terminal, the inquiry information indicating an inquiry about whether or not the second terminal is a terminal of an authorized member of the group;

an encrypted information receiving step of receiving predetermined encrypted information from the second terminal in response to the inquiry information sent in ~~the~~said inquiry information sending step;

a decryption trial step of trying ~~decrypting to decrypt~~ the received encrypted information by using the group public key of the second user;

an information judgment step of making a judgment ~~on~~as to whether or not decrypted information is appropriate ~~or not~~, when said decryption trial step successfully decrypts the received encrypted information; the decryption succeeds in the decryption trial step;

a participant judgment step of judging that the second terminal is a terminal of an authorized participant in the group, when the decrypted information is judged to be appropriate in ~~the~~said information judgment step;

an assignment information sending step of sending assignment information to the second terminal ~~when the second~~ whose user, that is, the second user who is the user of the second terminal, is judged to be an authorized participant, the assignment information indicating that ~~said the~~ second user is wished to be assigned as an issuer of the group who issues a participation certificate;

a public key receiving step of receiving the public key of the second user from the second terminal;

a public key judgment step of judging whether or not the received public key of the second user and the public key possessed by the first terminal match;

a permit generation step of generating a participation certificate issue permit indicating that authority to issue the participation certificate is granted to the second user; and

a permit sending step of sending the generated participation certificate issue permit to the second terminal; and

wherein said the steps B include:

an inquiry information receiving step of receiving the inquiry information from the first terminal;

a public key sending step of sending the public key of the second user to the first terminal; and

a permit receiving step of receiving the participation certificate issue permit from the first terminal.

22. (Currently Amended) The communication method according to Claim 21, wherein ~~the said~~ steps A further include:

a permission date specification step of specifying a date, month and year on which the public key of the second user was received; and

an expiration date determination step of determining an expiration date of the participation certificate issue permit, on the basis of ~~said the~~ specified date, month, and year; and

~~wherein said in the permit generation step comprises generating;~~ the participation certificate issue permit ~~is generated according to the public key of the second user and said the~~ expiration date.

23. (Currently Amended) A communication method for carrying out a communication between a first terminal and a second terminal on a network, wherein the first terminal possesses a public key of a group formed on the network and a pair of a private key and a public key of a first user who is a user of the first terminal, and the second terminal possesses a public key of the group, ~~the said~~ communication method comprising steps A executed by the first terminal and steps B executed by the second terminal,

wherein ~~the said~~ steps A include:

an inquiry information sending step of sending inquiry information to the second terminal, the inquiry information indicating an inquiry about whether or not the second terminal is a terminal of an authorized issuer of the group who has authority to issue a participation certificate;

a permit receiving step of receiving an encrypted participation certificate issue permit from the second terminal;

a decryption trial step of trying ~~decrypting to~~ decrypt the received participation certificate issue permit by using the public key of the group;

an information judgment step of making a judgment ~~on as to whether or not a~~ decrypted participation certificate issue permit is appropriate or not, when ~~the decryption succeeds in the said decryption trial step~~ successfully decrypts the received participation certificate;

an issuer judgment step of judging that the second terminal is a terminal of an authorized issuer of the group, when the decrypted participation certificate issue permit is judged to be appropriate in ~~the said~~ information judgment step;

a membership request sending step of sending membership request information to the second terminal judged to be the authorized issuer in ~~the said~~ issuer judgment step, the membership request information including information

indicating that the first user wishes to join the group and the public key of the first user; and

a participation certificate receiving step of receiving a participation certificate indicating that the first user has been approved to join the group from the second terminal; and

wherein said steps B include:

an inquiry information receiving step of receiving the inquiry information from the first terminal;

an encrypted information sending step of sending the encrypted participation certificate issue permit to the first terminal after the inquiry information is received;

a membership request receiving step of receiving the membership request information from the first terminal;

a participation certificate generation step of generating the participation certificate on the basis of the received membership request information; and

a participation certificate sending step of sending the generated participation certificate to the first terminal.

24. (Currently Amended) The communication method according to Claim 23,

wherein the said steps B further include:

a request date specification step of specifying a date, month and year on which the membership request information was received; and

an expiration date determination step of determining an expiration date of the participation certificate on the basis of said the specified date, month, and year; and

in the wherein said participation certificate generation step comprises generating;  
the participation certificate is ~~generated~~ according to the membership request information and said the expiration date.

25. (Currently Amended) The communication method according to claim 19, wherein the network is a P2P-peer to peer network.

26. (Currently Amended) A communication system comprising a first terminal and a second terminal that communicate with each other on a network, ~~the~~said first terminal possessing a public key of a group formed on the network and a pair of a private key and a public key of a first user who is a user of the first terminal, and ~~the~~said second terminal possessing a pair of a private key and a public key of the group,

wherein ~~the~~said first terminal includes:

an inquiry information sending unit operable to send inquiry information to ~~the~~said second terminal, the inquiry information indicating an inquiry about whether or not ~~the~~said second terminal is a terminal of an authorized member of the group;

an encrypted information receiving unit operable to receive predetermined encrypted information from ~~the~~said second terminal in response to the inquiry information sent by ~~the~~said inquiry information sending unit;

a decryption trial unit operable to try decrypting the received encrypted information by using the group public key;

an information judgment unit operable to make a judgment ~~on as to~~ whether or not decrypted information is appropriate ~~or not~~, when ~~the decryption succeeds in the~~ said decryption trial unit successfully decrypts the received encrypted information;

a manager judgment unit operable to judge that ~~the~~said second terminal is a terminal of an authorized manager of the group, when ~~the~~said information judgment unit judges that the decrypted information is appropriate;

a membership request sending unit operable to send membership request information to ~~the~~said second terminal judged to be the authorized manager by ~~the~~said manager judgment unit, the membership request information including information indicating that the first user wishes to join the group and the public key of the first user; and

a participation certificate receiving unit operable to receive a participation certificate indicating that the first user has been approved to join the group from ~~the~~said second terminal; and

~~the~~said second terminal includes:

an inquiry information receiving unit operable to receive the inquiry information from ~~the~~said first terminal;

an encrypted information sending unit operable to generate the encrypted information which has been encrypted according to the received inquiry information, and send the generated encrypted information to ~~the~~said first terminal;

a membership request receiving unit operable to receive the membership request information from ~~the~~said first terminal;

a participation certificate generation unit operable to generate the participation certificate on the basis of the received membership request information; and

a participation certificate sending unit operable to send the generated participation certificate to ~~the~~said first terminal.

27. (Currently Amended) The communication system according to Claim 26, wherein ~~the~~said second terminal further includes:

a request date specification unit operable to specify a date, month and year on which the membership request information was received; and

an expiration date determination unit operable to determine an expiration date of the participation certificate on the basis of the specified date, month, and year; and

~~the~~wherein said participation certificate generation unit ~~generates~~is operable to generate the participation certificate according to the membership request information and ~~said~~the expiration date.

28. (Currently Amended) A communication system comprising a first terminal and a second terminal that communicate with each other on a network, ~~the~~said first terminal possessing a pair of a private key and a public key of a group formed on the network and a public key of a second user who is a user of the second terminal, and ~~the~~said second terminal possessing a public key of the group,

wherein ~~the~~said first terminal includes:

an inquiry information sending unit operable to send inquiry information to ~~the~~said second terminal, the inquiry information indicating an inquiry about whether or not ~~the~~said second terminal is a terminal of an authorized member of the group;

an encrypted information receiving unit operable to receive predetermined encrypted information from ~~the~~said second terminal in response to the inquiry information sent by ~~the~~said inquiry information sending unit;

a decryption trial unit operable to try decrypting the received encrypted information by using the public key of the second user;

an information judgment unit operable to make a judgment ~~on~~as to whether or not decrypted information is appropriate ~~or not~~, when ~~the decryption succeeds in the~~said decryption trial unit successfully decrypts the received encrypted information;

a participant judgment unit operable to judge that ~~the~~said second terminal is a terminal of an authorized participant in the group, when ~~the~~said information judgment unit judges that the decrypted information is appropriate;

an assignment information sending unit operable to send assignment information to ~~the~~said second terminal when the second ~~whose user, who is the user of said second terminal that is, the second user~~ is judged to be an authorized participant, the assignment information indicating that the second user is wished to be assigned as an issuer of the group who issues a participation certificate;

a public key receiving unit operable to receive the public key of the second user from ~~the~~said second terminal;

a public key judgment unit operable to judge whether or not the received public key of the second user and the public key possessed by ~~the~~said first terminal match;

a permit generation unit operable to generate a participation certificate issue permit indicating that authority to issue the participation certificate is granted to the second user; and

a permit sending unit operable to send the generated participation certificate issue permit to ~~the~~said second terminal; and

~~the~~ wherein said second terminal includes:

an inquiry information receiving unit operable to receive the inquiry information from ~~the~~ said first terminal;

a public key sending unit operable to send the public key of the second user to ~~the~~ said first terminal; and

a permit receiving unit operable to receive the participation certificate issue permit from ~~the~~ said first terminal.

29. (Currently Amended) The communication system according to Claim 28, wherein said first terminal further includes:

a permission date specification unit operable to specify a date, month and year on which the public key of the second user was received; and

an expiration date determination unit operable to determine an expiration date of the participation certificate issue permit, on the basis of ~~said~~ the specified date, month, and year; and

~~the~~ wherein said permit generation unit ~~generates~~ is operable to generate the participation certificate issue permit according to the public key of the second user and ~~said~~ the expiration date.

30. (Currently Amended) A communication system comprising a first terminal and a second terminal that communicate with each other on a network, ~~the~~ said first terminal possessing a public key of a group formed on the network and a pair of a private key and a public key of a first user who is a user of ~~the~~ said first terminal, and ~~the~~ said second terminal possessing a public key of the group,

wherein ~~the~~ said first terminal includes:

an inquiry information sending unit operable to send inquiry information to ~~the~~ said second terminal, the inquiry information indicating an inquiry about whether or not ~~the~~ said second terminal is a terminal of an authorized issuer of the group who has authority to issue a participation certificate;

a permit receiving unit operable to receive an encrypted participation certificate issue permit from ~~the~~ said second terminal;



a decryption trial unit operable to try decrypting the received participation certificate issue permit by using the public key of the group;

an information judgment unit operable to make a judgment ~~on~~ as to whether or not a decrypted participation certificate issue permit is appropriate ~~or not~~, when ~~the decryption succeeds in the~~ said decryption trial unit successfully decrypts the received participation certificate issue permit;

an issuer judgment unit operable to judge that ~~the~~ said second terminal is a terminal of an authorized issuer of the group, when ~~the~~ said information judgment unit judges that the decrypted participation certificate issue permit is appropriate;

a membership request sending unit operable to send membership request information to ~~the~~ said second terminal judged to be the authorized issuer by ~~the~~ said issuer judgment unit, the membership request information including information indicating that the first user wishes to join the group and the public key of the first user; and

a participation certificate receiving unit operable to receive a participation certificate indicating that the first user has been approved to join the group from ~~the~~ said second terminal; and  
wherein said ~~the~~ second terminal includes:

an inquiry information receiving unit operable to receive the inquiry information from ~~the~~ said first terminal;

an encrypted information sending unit operable to send the encrypted participation certificate issue permit to ~~the~~ said first terminal after receiving the inquiry information;

a membership request receiving unit operable to receive the membership request information from ~~the~~ said first terminal,

a participation certificate generation unit operable to generate the participation certificate on the basis of the received membership request information; and

a participation certificate sending unit operable to send the generated participation certificate to ~~the~~ said first terminal.

31. (Currently Amended) The communication system according to Claim 30, wherein ~~the said~~ second terminal further includes:

an request date specification unit operable to specify a date, month and year on which the membership request information was received; and

an expiration date determination unit operable to determine an expiration date of the participation certificate on the basis of ~~said the~~ specified date, month, and year; and

wherein said the participation certificate generation unit generates-is operable to generate the participation certificate according to the membership request information and said the expiration date.

32. (Currently Amended) The communication system according to claim 26, wherein the network is a ~~P2P~~peer to peer network.

33. (Currently Amended) A program, recorded on a computer-readable medium, for a terminal apparatus that communicates with another terminal apparatus on a network, wherein the first terminal apparatus possesses a public key of a group formed on the network, ~~the said~~ program comprising:

an inquiry information sending step of sending inquiry information to ~~said another the other~~ terminal apparatus, the inquiry information indicating an inquiry about whether or not ~~said another the other~~ terminal apparatus is a terminal apparatus of an authorized member of the group;

an encrypted information receiving step of receiving predetermined encrypted information from ~~said another the other~~ terminal apparatus in response to the inquiry information sent in ~~the said~~ inquiry information sending step;

a decryption trial step of trying ~~decrypting to decrypt~~ the received encrypted information by using the group public key;

an information judgment step of making a judgment ~~on as to whether or not~~ decrypted information is appropriate ~~or not~~, when ~~the decryption succeeds in the said~~ decryption trial step successfully decrypts the received encrypted information; and

a terminal judgment step of judging that ~~said another~~ the other terminal apparatus is a terminal apparatus of an authorized member of the group, when the decrypted information is judged to be appropriate in ~~the~~ said information judgment step.

34. (Currently Amended) The program according to Claim 33, wherein the network is a P2P-peer to peer network.

35-36. (Cancelled)

37. (Currently Amended) The communication method according to claim 21, wherein the network is a P2P-peer to peer network.

38. (Currently Amended) The communication method according to claim 23, wherein the network is a P2P-peer to peer network.

39. (Currently Amended) The communication system according to claim 28, wherein the network is a P2P-peer to peer network.

40. (Currently Amended) The communication system according to claim 30, wherein the network is a P2P-peer to peer network.